UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/878,319	06/12/2001	Mark Crosbie	10004512-1	2127

7590 04/20/2005

IP Administration
Legal Department, M/S 35
HEWLETT-PACKARD COMPANY
P.O. Box 272400
Fort Collins, CO 80528-9599

EXAMINER	
PARTHASARATHY, PRAMILA	
ART UNIT	**PAPER NUMBER**
2136	

DATE MAILED: 04/20/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/878,319	CROSBIE ET AL.	
	Examiner	Art Unit	
	Pramila Parthasarathy	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 January 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-10,12-32 and 35-43* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10,12-32 and 35-43* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to remarks and amendments filed on January 18, 2005. Applicant has amended Claims 1, 29 and 31. Claims 11, 33, 34 and 44 – 48 were cancelled and no new claims were added. Therefore, presently pending Claims are 1 – 10, 12 - 32 and 35 – 43.

Claim Objections

2. Objection to Claim 35 is hereby withdrawn.

Specification

3. The substitute specification filed on 1/18/2005 has not been entered because it does not conform to 37 CFR 1.125(b) and (c) because: Amendment to specification on page 1 recites " Please amend the sixth paragraph beginning on page 17 of the current specification as follows:

A secure communications link. The host-based IDS needs a means of stopping an attacker from observing the traffic between its components and possibly sending false data to disrupt its operations. An encrypted link can prevent this from happening. ", but does not contain any text marked to amend.

4. A substitute specification including the claims is required pursuant to 37 CFR 1.125(a) because the above request for amending the sixth paragraph for page 17 (original specification), does not explicitly show the text that needs to be amended.

5. A substitute specification must not contain new matter. The substitute specification must be submitted with markings showing all the changes relative to the immediate prior version of the specification of record. The text of any added subject matter must be shown by underlining the added text. The text of any deleted matter must be shown by strike-through except that double brackets placed before and after the deleted characters may be used to show deletion of five or fewer consecutive characters. The text of any deleted subject matter must be shown by being placed within double brackets if strike-through cannot be easily perceived. An accompanying clean version (without markings) and a statement that the substitute specification contains no new matter must also be supplied. Numbering the paragraphs of the specification of record is not considered a change that must be shown.

Response to Arguments

6. Applicant's arguments filed on January 18, 2005, have been fully considered but they are not persuasive for the following reasons:

7. Remarks contain many errors with respect to Claim numbers that are discussed. For example, with respect to Claim 28, Claim 28 is dependent on Claim 1 wherein, the remarks discloses Claim 28 as incorporating the now cancelled claims 33 and 34, in fact it should be Claim 29. Examiner reads that as Claims 33 and 34 now incorporated into independent Claim 29. Remarks also mentions claim 34 as dependent on 29 (Page 20), in fact Claim 34 has been cancelled.

8. Regarding amended independent Claim 1, applicant argued that the cited prior art Moran (U.S. Patent Number 6,647,400) does not disclose "reading of kernel records", "reformatting the read kernel records into a different format, wherein the different format is a memory mapped file;" and "parsing and comparing the kernel records against a template". This argument is not persuasive. Moron discloses reading of kernel records (Column 11 lines 15 – 54), wherein the intrusion system search the file system/directories reformatting the kernel records in a different format (e.g. dump formats), wherein the different format is a memory mapped file (Column 27 lines 37 – 39 and Column 29 lines 4 – 52) and parsing and comparing the kernel records against a template (Column 18 lines 6 – 58), wherein the analysis engine performs parsing and comparing the kernel records. Furthermore, Moron discloses the analysis engine cross-checking the kernel records against a template (file signatures) (Column 32 lines 44 – 58).

9. Regarding amended independent Claim 29, applicant argued that Moran does not disclose, "if a directory is specifically excluded and a file in the specifically excluded directory is specifically included the file is monitored" and "the predetermined set of files includes a system kernel file and system kernel configuration files". This argument is not persuasive. Moron discloses that the intrusion system can be configured to monitor a file that is included in the specifically excluded directory (Column 32 line 44 – Column 33 line 62), wherein the analysis engine monitors the files that are not specific to an individual host and wherein the files includes a system kernel file and system kernel configuration file (e.g.: .config, .log, /etc and /var/log).

10. Therefore, the examiner respectfully asserts that the cited prior art does teach or suggest the amended subject matter "the different format is a memory mapped file", "if a directory is specifically excluded and a file in the specifically excluded directory is specifically included the file is monitored" and "the predetermined set of files includes a system kernel file and system kernel configuration files", broadly recited in the amended independent claims 1 and 29. The dependent claims 2 – 10, 12 – 28, 30 - 32 and 35 – 43 are rejected at least by virtue of their dependency on the dependent claims and by other reason set forth in this office action. Accordingly, the rejection for the pending claims 1 – 10, 12 - 32 and 35 – 43 is respectfully maintained.

Claim Rejections - 35 USC § 102

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

11. Claims 1 – 10, 12 – 32 and 35 – 43 are rejected under 35 U.S.C. 102(e) as being anticipated by Moran (U.S. Patent Number 6,647,400).

12. Regarding Claim 1, Moran teaches and describes a method of detecting intrusions using a host-based intrusion system (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), comprising:

reading kernel records (Column 7 line 39 – Column 8 line 20 and Column 11 lines 15 – 54);

reformatting each of the read kernel records into a different format, wherein the different format is a memory mapped file (Column 9 line 54 – Column 10 line 32, Column 27 lines 37 – 39 and Column 29 lines 4 – 52);

parsing the records and comparing the parsed records against one or more templates (Column 18 lines 6 – 58).

13. Regarding Claim 29, Moran teaches and describes a method of detecting changes to critical files/directories (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), comprising:

monitoring a predetermined set of files for modifications (Column 8 lines 6 – Column 10 line 55 and Column 11 lines 16 – 54);

monitoring a predetermined set of directories for modifications (Column 8 line 6 – Column 10 line 55 and Column 11 lines 16 – 54);

generating an alert for each occurrence of a modification of a monitored file, wherein if a directory is specifically excluded and a file in the specifically excluded directory is specifically included the file is monitored, and wherein the predetermined set of files includes a system kernel file and system kernel configuration files (Column 10 lines 14 – 55; Column 13 lines 1 – 31 and Column 35 lines 9 – 42); and

generating an alert for each occurrence of a modification of a monitored directory (Column 10 lines 14 – 55; Column 13 lines 1 – 31, Column 32 line 44 – Column 33 line 62 and Column 35 lines 9 – 42).

14. Claim 2 is rejected as applied above in rejecting Claim 1. Furthermore, Moran teaches and describes a method of detecting intrusions using a host-based intrusion system (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein the kernel audit logs includes information about each system call (Column 8 line 6 – 46 and Column 9 lines 12 – 65).

15. Claim 4 is rejected as applied above in rejecting Claim 1. Furthermore, Moran teaches and describes a method of detecting intrusions using a host-based intrusion

system (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), comprising monitoring system log files (Column 10 lines 14 – 55).

16. Claim 5 is rejected as applied above in rejecting Claim 1. Furthermore, Moran teaches and describes a method of detecting intrusions using a host-based intrusion system (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), comprising a system call (Column 10 lines 33 – 47).

17. Claim 6 is rejected as applied above in rejecting Claim 1. Furthermore, Moran teaches and describes a method of detecting intrusions using a host-based intrusion system (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein the system call was initiated by a library call (Column 10 lines 33 – 47 and Column 13 lines 1 – 11).

18. Claim 8 is rejected as applied above in rejecting Claim 1. Furthermore, Moran teaches and describes a method of detecting intrusions using a host-based intrusion system (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), comprising determining that an intrusion has occurred and generating an alert message (Column 8 lines 6 – 46).

19. Claim 9 is rejected as applied above in rejecting Claim 1. Furthermore, Moran teaches and describes a method of detecting intrusions using a host-based intrusion

system (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), comprising encrypting information sent between the host-based intrusion system and a network (Column 16 lines 15 – 29).

20. Claim 10 is rejected as applied above in rejecting Claim 1. Furthermore, Moran teaches and describes a method of detecting intrusions using a host-based intrusion system (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), comprising displaying an alert message that an intrusion has occurred (Column 8 lines 6 – 46 and Column 10 lines 14 – 55).

21. Claim 14 is rejected as applied above in rejecting Claim 1. Furthermore, Moran teaches and describes a method of detecting intrusions using a host-based intrusion system (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein the one or more templates is a modification of files/directories template (Column 18 lines 6 – 58 and Column 31 lines 31 – 40).

22. Claim 15 is rejected as applied above in rejecting Claim 1. Furthermore, Moran teaches and describes a method of detecting intrusions using a host-based intrusion system (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein the one or more templates is a change to log files template (Column 2 lines 40 – 47; Column 10 lines 14 – 55 and Column 11 lines 41 – 54).

23. Claim 16 is rejected as applied above in rejecting Claim 1. Furthermore, Moran teaches and describes a method of detecting intrusions using a host-based intrusion system (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein the one or more templates is a SetUID files template (Column 9 lines 33 – 47 and Column 12 lines 46 – 67).

24. Claim 17 is rejected as applied above in rejecting Claim 1. Furthermore, Moran teaches and describes a method of detecting intrusions using a host-based intrusion system (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein the one or more templates is a creation of world-writables template (Column 11 line 55 – Column 12 line 67).

25. Claim 18 is rejected as applied above in rejecting Claim 1. Furthermore, Moran teaches and describes a method of detecting intrusions using a host-based intrusion system (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein the one or more templates is a repeated failed logins template (Column 19 line 49 – Column 20 line 67).

26. Claim 19 is rejected as applied above in rejecting Claim 1. Furthermore, Moran teaches and describes a method of detecting intrusions using a host-based intrusion system (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein the

one or more templates is a repeated failed SU commands template (Column 23 lines 14 – 46 and Column 25 lines 15 – 45).

27. Claim 20 is rejected as applied above in rejecting Claim 1. Furthermore, Moran teaches and describes a method of detecting intrusions using a host-based intrusion system (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein the one or more templates is a race conditions attack template (Column 12 lines 31 – 67).

28. Claim 21 is rejected as applied above in rejecting Claim 1. Furthermore, Moran teaches and describes a method of detecting intrusions using a host-based intrusion system (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein the one or more templates is a buffer overflow attacks template (Column 9 lines 33 – 47 and Column 33 line 64 – Column 34 line 42).

29. Claim 22 is rejected as applied above in rejecting Claim 1. Furthermore, Moran teaches and describes a method of detecting intrusions using a host-based intrusion system (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein the one or more templates is a modification of another user's file template (Column 18 lines 6 – 58 and Column 31 lines 31 – 40).

30. Claim 23 is rejected as applied above in rejecting Claim 1. Furthermore, Moran teaches and describes a method of detecting intrusions using a host-based intrusion

system (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein one or more templates is a monitor for the start of interactive sessions template (Column 38 lines 31 – 51).

31. Claim 24 is rejected as applied above in rejecting Claim 1. Furthermore, Moran teaches and describes a method of detecting intrusions using a host-based intrusion system (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein the one or more template is a monitor logins/logouts template (Column 23 lines 14 – 46 and Column 24 lines 33 – 41).

32. Claim 25 is rejected as applied above in rejecting Claim 1. Furthermore, Moran teaches and describes a method of detecting intrusions using a host-based intrusion system (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein the one or more templates is chosen from the group including:

a modification of files/directories template (Column 18 lines 6 – 58 and Column 31 lines 31 – 40);

a change to log files template (Column 2 lines 40 – 47; Column 10 lines 14 – 55 and Column 11 lines 41 – 54);

a SetUID files template (Column 9 lines 33 – 47 and Column 12 lines 46 – 67);

a creation of world-writables template (Column 11 line 55 – Column 12 line 67);

a repeated failed logins template (Column 19 line 49 – Column 20 line 67);

a repeated failed SU commands template (Column 23 lines 14 – 46 and Column 25 lines 15 – 45);

a race conditions attack template (Column 12 lines 31 – 67);

a buffer overflow attacks template (Column 9 lines 33 – 47 and Column 33 line 64 – Column 34 line 42);

a modification of another user's file template (Column 18 lines 6 – 58 and Column 31 lines 31 – 40);

a monitor for the start of interactive sessions template (Column 38 lines 31 – 51); and

a monitor logins/logouts template (Column 23 lines 14 – 46 and Column 24 lines 33 – 41).

33. Claim 26 is rejected as applied above in rejecting Claim 1. Furthermore, Moran teaches and describes a method of detecting intrusions using a host-based intrusion system (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein the kernel records are read from different computers (Column 10 lines 14 – 55 and Column 17 line 50 – Column 18 line 5).

34. Claim 27 is rejected as applied above in rejecting Claim 1. Furthermore, Moran teaches and describes a method of detecting intrusions using a host-based intrusion system (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein parsed records are compared against the one or more templates using at least one

correlator (Column 11 lines 16 – 28; Column 23 lines 14 – 46 and Column 24 lines 47 – 51).

35. Claim 28 is rejected as applied above in rejecting Claim 1. Furthermore, Moran teaches and describes a method of detecting intrusions using a host-based intrusion system (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein said parsing step compares the parsed records against one or more templates simultaneously (Column 32 line 44 – Column 33 line 11).

36. Claim 30 is rejected as applied above in rejecting Claim 29. Furthermore, Moran teaches and describes a method of detecting changes to critical files/directories (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), comprising:

determining which files to monitor of all files on a computer to form the predetermined set of files; determining which directories to monitor of all directories on a computer to form the predetermined set of directories (Column 8 lines 6 – 46; Column 11 line 16 – Column 12 line 30; Column 23 lines 14 – 46 and Column 32 line 44 – Column 33 line 62).

37. Claim 31 is rejected as applied above in rejecting Claim 29. Furthermore, Moran teaches and describes a method of detecting changes to critical files/directories (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), comprising, for each said determining step, specifically including a file or directory, specifically excluding a file or

directory or not specifically including or excluding a file or directory (Column 8 lines 6 – 46; Column 11 line 16 – Column 12 line 30; Column 23 lines 14 – 46 and Column 32 line 44 – Column 33 line 62).

38. Claim 32 is rejected as applied above in rejecting Claim 29. Furthermore, Moran teaches and describes a method of detecting changes to critical files/directories (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein a file or directory which is not specifically included or excluded is monitored (Column 8 lines 6 – 46; Column 11 line 16 – Column 12 line 30; Column 23 lines 14 – 46 and Column 32 line 44 – Column 33 line 62).

39. Claim 35 is rejected as applied above in rejecting Claim 29. Furthermore, Moran teaches and describes a method of detecting changes to critical files/directories (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein the predetermined set of files includes /stand/vmunix, /stand/kernel and stand/bootconf (Column 32 line 44 – Column 33 line 62).

40. Claim 36 is rejected as applied above in rejecting Claim 29. Furthermore, Moran teaches and describes a method of detecting changes to critical files/directories (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein the predetermined set of files includes files defining the users on a system and files used to

create accounts (Column 11 line 55 – Column 12 line 30; Column 20 lines 36 – 67 and Column 25 line 15 – Column 26 line 45).

41. Claim 37 is rejected as applied above in rejecting Claim 29. Furthermore, Moran teaches and describes a method of detecting changes to critical files/directories (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein the predetermined set of files includes /etc/passwd and /etc/group (Column 11 line 55 – Column 12 line 30; Column 20 lines 36 – 67 and Column 32 line 49 – Column 33 line 11).

42. Claim 38 is rejected as applied above in rejecting Claim 29. Furthermore, Moran teaches and describes a method of detecting changes to critical files/directories (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein the predetermined set of files includes files which control what network services are running and which controls programs used to fulfill service requests (Column 19 lines 28 – 65 and Column 21 line 1 – 14).

43. Claim 39 is rejected as applied above in rejecting Claim 29. Furthermore, Moran teaches and describes a method of detecting changes to critical files/directories (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein the predetermined set of files includes /etc/inetd.conf (Column 11 line 55 – Column 12 line 30; Column 20 lines 36 – 67 and Column 32 line 49 – Column 33 line 11).

Claim 40 is rejected as applied above in rejecting Claim 29. Furthermore, Moran teaches and describes a method of detecting changes to critical files/directories (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein the predetermined set of files includes files which are used to control the remote access of the user root without requiring a password (Column 23 lines 14 – 46 and Column 35 lines 9 – 63).

44. Claim 41 is rejected as applied above in rejecting Claim 29. Furthermore, Moran teaches and describes a method of detecting changes to critical files/directories (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein the predetermined set of files includes/.rhosts and /.shosts (Column 9 lines 1 – 22 and Column 35 lines 9 – 63).

45. Claim 42 is rejected as applied above in rejecting Claim 29. Furthermore, Moran teaches and describes a method of detecting changes to critical files/directories (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein the set of files specifically excluded includes temporary files created by a program view (Column 27 line 32 – Column 29 line 52).

46. Claim 43 is rejected as applied above in rejecting Claim 29. Furthermore, Moran teaches and describes a method of detecting changes to critical files/directories (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein the

predetermined set of directories includes Jbin, /sbin and /usr/bin (Column 36 line 7 – Column 37 line 7 and Column 39 lines 43 – 65).

47. Claim 3 is rejected as applied above in rejecting Claim 2. Furthermore, Moran teaches and describes a method of detecting intrusions using a host-based intrusion system (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein the kernel audit logs includes information about each system call (Column 8 line 6 – 46 and Column 9 lines 12 – 47).

48. Claim 13 is rejected as applied above in rejecting Claim 2. Furthermore, Moran teaches and describes a method of detecting intrusions using a host-based intrusion system (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), comprising converting the kernel records into an ASCII format for comparison against the one or more templates (Column 10 lines 14 – 53; Column 11 lines 29 – 40 and Column 13 lines 26 – 31).

49. Claim 7 is rejected as applied above in rejecting Claim 3. Furthermore, Moran teaches and describes a method of detecting intrusions using a host-based intrusion system (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), comprising storing each system call in a circular buffer (Column 8 line 6 – 46; Column 9 lines 12 – 47).

50. Claim 12 is rejected as applied above in rejecting Claim 4. Furthermore, Moran teaches and describes a method of detecting intrusions using a host-based intrusion system (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), comprising converting the system log files into an ASCII format for comparison against the one or more templates (Column 9 line 54 – Column 10 line 32).

Conclusion

52. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTO Form 892.

53. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

54. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Pramila Parthasarathy whose telephone number is 571-272-3866. The examiner can normally be reached on 8:00a.m. To 5:00p.m.. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-232-3795. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR only. For more information about the PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Pramila Parthasarathy
April 06, 2005.